REMARKS/ARGUMENTS

Claims 1-38 have been rejected. Claims 39-42 have been added. Claims 1-42 are pending in the application.

35 U.S.C. § 102 - Ansell

Claims 1-16 stand rejected under 35 U.S.C. §102(e) as being anticipated by Ansell et al. (USPN 6,367,019) (hereinafter "Ansell"). Applicant respectfully submits that Claims 1-16 are not anticipated by Ansell.

Claim 1 recites:

> A method comprising:
> randomly retrieving data from a removable data storage medium, wherein the removable data storage medium contains an executable application program;
> comparing the retrieved data to corresponding verification data, wherein the verification data is known to be valid; and
> allowing execution of the executable application program if the retrieved data matches the corresponding verification data.

Ansell describes a system for providing copy security for portable music. To reject "randomly retrieving data from a removable data storage medium" in Claim 1, the Office Action cites Claims 44-48 and col. 2, lines 5-14 and 28-35 in Ansell. (Office Action, paragraph 2.3). Claim 44 of Ansell recites:

> A computer readable medium useful in association with a computer which includes a processor and a memory, the computer readable medium including computer instructions which are configured to cause the computer to access subject data from a storage medium by a selected data access device by:
> retrieving key identification data from the storage medium;

determining that the key identification data corresponds to data secretly held by the selected data access device;

retrieving encrypted subject data from the storage medium; and

decrypting the encrypted subject data using the data secretly held by the selected data access device as an encryption key to form the subject data;

wherein the key identification data is formed from the encryption key; and

wherein the encryption key is not directly determinable from data stored on the storage medium including the key identification data and the encrypted subject data.

Thus, according to Claim 44 of Ansell, key identification data is specifically retrieved from the storage medium so that it can be verified against some secret data. If the key identification data is verified, the data in the storage medium is decrypted using the secret data as the decryption key. However, Claim 44 of Ansell does not describe "randomly retrieving data from a removable data storage medium" as recited in Claim 1. In contrast, the method of Ansell specifically retrieves a particular type of data from the storage medium, namely the "key identification data".

Claims 45-48 of Ansell and col. 2, lines 5-14 and 28-35 merely add further explanation and limitations to the basic method in Claim 44 of Ansell discussed above. These additional materials do not remedy the deficiencies of the method described in Claim 44 of Ansell.

For the reasons stated above, Applicant respectfully submits that Claim 1 is allowable over Ansell. Given that Claims 2-9 depend from Claim 1, Claims 2-9 are also allowable over Ansell for at least the same reasons.

Claim 10 recites:

A method comprising:

randomly retrieving data from a removable data storage medium, wherein the removable data storage medium contains at least one file of audio data;

comparing the retrieved data to corresponding verification data, wherein the verification data is known to be valid; and

allowing access to the at least one file of audio data if the retrieved data matches the corresponding verification data.

Claim 10 stands rejected under essentially the same reasons given by the Office Action for rejecting Claim 1. Thus, independent Claim 10 and dependent Claims 11-16 are allowable over Ansell for at least the same reasons.

35 U.S.C. § 102 - Bharat

Claims 17-38 stand rejected under 35 U.S.C. §102(e) as being anticipated by Bharat et al. (USPN 6,577,735) (hereinafter "Bharat"). Applicant respectfully submits that Claims 17-38 are not anticipated by Bharat.

Claim 17 recites:

A method of verifying the presence of a legitimate removable data storage medium, the method comprising:

randomly retrieving at least one data block from the removable data storage medium, wherein the removable data storage medium contains a plurality of data blocks;

comparing the retrieved data block to a corresponding verification data block, wherein the verification data block is known to be valid; and

determining that a legitimate removable data storage medium is present if the retrieved data block matches the corresponding verification data block.

Bharat describes a system and method for backing-up data stored on a portable audio player. In particular, Bharat discloses

> A system creates an encrypted backup copy of the compressed audio data downloaded onto a portable audio player. When a user loads a portable audio player with audio data from a CD inserted into a computer's CD-ROM drive, the system creates an encrypted copy of the compressed audio data and stores the encrypted copy on the computer's hard disk. The encrypted copy cannot be used without a cryptographic key, but the system discards the cryptographic key once the encrypted copy of the audio data is stored. To extract usable audio data from the encrypted back-up copy, it is necessary to re-insert the original CD and regenerate the cryptographic key. Once the cryptographic key is regenerated, the encrypted audio data can be decrypted and re-loaded onto the portable audio player. (Bharat, Abstract)

Thus, Bharat discloses a system for creating a back-up copy of compressed audio data from a CD and encrypting the back-up copy with a cryptographic key generated from the CD. To access the back-up copy, the CD is required to regenerate the cryptographic key. However, the system in Bharat does not disclose "randomly retrieving at least one data block from the removable data storage medium" as recited in Claim 17. Rather, Bharat requires specifically retrieving certain data from the CD to regenerate the cryptographic key.

To reject Claim 17, the Office Action cites Bharat at col. 6, lines 51 through col. 7, line 4 and col. 8 lines 4-23). (Office Action, paragraph 3.1) These materials describe a header of a back-up audio data file that can be used to verify a CD. In particular, the materials include

> Header 410 may also include a "certificate" that can be used to verify the accuracy of a subsequent decryption operation, as described below, and can also be used to determine whether the original CD 210 has been re-inserted into CD-ROM drive 208. For instance, the certificate may consist of a predefined datum, such as the string "Compaq Authenticity Certificate" encrypted with the encryption key derived from the audio CD data. Alternatively, the certificate may contain encrypted information

derived from the audio CD, such as information about the lengths of the audio tracks on the audio CD. (Bharat, col. 6, line 61 to col. 7, line 4)

Bharat discloses that the header of the back-up audio file may include a certificate that can be used to verify the data stored in a CD. However, the certificate in the header of the back-up audio file would have to be compared to the certificate in the CD, which is retrieved specifically, not randomly.

For the reasons stated above, Applicant respectfully submits that Claim 17 is allowable over Bharat. Given that Claims 18-23 depend from Claim 17, Claims 18-23 are also allowable over Bharat for at least the same reasons.

Claim 24 recites:

> A verification system comprising:
> a data reading device to read data from a removable data storage medium; and
> a verification module coupled to the data reading device, wherein the verification module is to randomly retrieve data from the removable data storage medium and compare the retrieved data to corresponding verification data that is known to be valid, and wherein the verification module is further to determine that a legitimate removable data storage medium is present if the retrieved data matches the corresponding verification data.

Claim 38 recites:

> One or more computer-readable media having stored thereon a computer program comprising the following steps:
> randomly retrieving data from a removable data storage medium;
> comparing the retrieved data to corresponding verification data, wherein the verification data is known to be valid; and
> determining that a legitimate removable data storage medium is present if the retrieved data matches the corresponding verification data.

As discussed above, Bharat does not disclose randomly retrieving data from the removable data storage medium. Rather, Bharat discloses specifically retrieving certain data from a CD and comparing the retrieved data to the data in a back-up audio file. Thus, independent Claims 24 and 30 and dependent Claims 26-29 and 31-33 are also allowable for at least the same reasons.

Claim 34 recites:

> A method comprising:
> randomly selecting a data block identifier, wherein the data block identifier identifies a particular data block on a removable data storage medium;
> issuing a challenge and the data block identifier to a data reading device, wherein the removable data storage medium is readable by the data reading device;
> the data reading device hashing the challenge with the data contained in the particular data block on the removable data storage medium;
> receiving the result of the hashing operation;
> comparing the result of the hashing operation to corresponding verification data, wherein the verification data is known to be valid; and
> determining that the removable data storage medium is legitimate if the result of the hashing operation matches the corresponding verification data.

To reject Claim 34, the Office Action cites col. 6, line 5 through col. 7, line 40. These seven paragraphs of materials describe a procedure for encrypting back-up audio files. The materials also disclose a header of a back-up audio data file that can be used to verify a CD, as discussed above. However, none of these materials describes the method recited in Claim 34.

The Office Action also cites materials at col. 8, lines 1-23 in Bharat. These materials disclose a procedure for including the serial number of an authorized portable audio player into an archive file and using the serial number to prevent the archive file from being downloaded to an unauthorized audio player. However, the cited materials do not describe and are not related to the method recited in Claim 34.

For the above reasons, Applicant respectfully submits that Claim 34 is not anticipated by Bharat and is allowable. Given that Claims 35-38 depend from Claim 34, Claims 35-38 are also allowable for at least these reasons.

New Claims

New Claims 39-42 are added herein. Applicant respectfully submits that Claims 39-42 are allowable for at least the reasons discussed above.

Conclusion

Claims 1-42 are now in condition for allowance. Applicant respectfully requests the issuance of the subject application. Should any matter in this case remain unresolved, the undersigned attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Respectfully Submitted,

Date: 1/22/2004

By: _____

Thomas Wong
Reg. No. 48,577
(206) 315- 4001 X106